Cyber Espionage:
Is the United States getting more than its giving?

Revised: 03/05/2010

While there has been an abundance of talk about the importance of securing cyberspace, the U.S. Government's actions and results to date do not seem commensurate with the oratory. Despite the numerous studies and recommendations, ongoing planning, increased spending, and a host of other activities over the last several years, there has been little significant progress made in securing cyberspace as a result of U.S. Government action. According to the recommendations from recent cybersecurity studies (e.g. Melissa Hathaway's federal cybersecurity review, the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency), progress would include: the appointment of a federal cybersecurity coordinator reporting to the President; a national strategy for defending cyber-infrastructure; the establishment of cyber performance metrics; new legislation and policies that would allow for cyber issues to be addressed across agencies; cybersecurity public awareness, education and training campaigns; the promotion of international cybersecurity through international partnerships; better information sharing between government and the private sector; the development of a cybersecurity incident response plan; and the development of an identity management system that takes privacy and civil liberty concerns into consideration.[1]

An obvious question is:

> *Why doesn't the U.S. have more to show for the U.S. Government's clearly stated intentions to secure cyberspace?*

Admittedly, the U.S. Government (USG) has a growing list of "priorities" – fighting terrorism, the economy, healthcare, climate change, unemployment, and others. These priorities alone do not explain the lack of USG cybersecurity progress considering the size of the USG, the number of Departments, advisors/czars and other civil servants, the amount of spending that has occurred over the last several years, and the U.S. influence on nations, businesses, and individuals. Cybersecurity has clearly become a stated Presidential and national priority, so; Is there more to the U.S. Government's lack of progress in securing cyberspace?

This paper attempts to tie together information, as reported by open-source media, which may provide insight into why the USG does not appear to "walk the talk" when it comes to cyberspace security.

Key questions to be considered include:

> *Is the U.S. Government gaining more from its own cyber espionage activities than it is losing via other nations successful attempts to steal U.S. information?*

> *Is it possible the U.S. Government does not have a more secure cyberspace and/or stop more cyber espionage [2] attempts because doing so would actually decrease the U.S. advantage(s)?*

The United States is being "attacked" -- both government and industry. The Department of Homeland Security's Computer Emergency Readiness Team reports that North Korean hackers attacked multiple U.S. government agencies with a widespread computer attack beginning on July 4, 2009. Several federal systems were shut down for a time. The hackers used a denial of service (DOS) attack that caused a "major outage" of U.S. and South Korean government web sites.[3] The attack was large enough to affect the U.S. Treasury Department, Secret

[1] http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=217700860
[2] Espionage is a lively undertaking among powerful states – in military technology, commercial secrets, designs and research formulae, trade and capital, even government negotiating positions on any imaginable issue. It has gotten livelier in the past decade because the computer cuts out laborious and often clumsy on-site intervention.; http://www.chinapost.com.tw/commentary/the-china-post/special-to-the-china-post/2010/01/30/242920/Cyber-spying.htm
[3] http://military.rightpundits.com/2009/07/08/north-korean-cyber-attack-widespread-computer-attack-on-us-government-agencies/

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

Service, Federal Trade Commission, Stock Exchange, the White House and the Transportation Department.[4] In addition to these DOS attacks, North Korean hackers were recently able to access a secret U.S-South Korean plan to defend the Korean peninsula in case of war.[5] In addition, reports from the U.S.-China Economic and Security Review Commission claim that China is becoming "increasingly aggressive in its espionage efforts to obtain U.S. secrets and technology to benefit its military."[6] There have been multiple examples of this increasing aggression. In 2008, Chinese hackers allegedly gained access to both the Obama and McCain campaigns' computer systems. Wang Baodong, the spokesman at the Chinese Embassy in Washington, continues to dismiss accusations against China as "unwarranted, irresponsible and misleading,"[7] but experts warn that Chinese hackers are regularly gathering intelligence[8] in case of a war. Intelligence officials claim that both Russia and China are "able to target and disrupt elements of the U.S. information infrastructure."[9]

Matt Moynahan, CEO of application security firm Veracode, says that all government and organized non-government actors are engaging in cyber espionage. Jody Westby, CEO of consulting firm Global Cyber Risk, says "China, Russia, North Korea, Iran, Israel, France, the United States and the United Kingdom are widely known to possess state-of-the-art cyber espionage know-how used for economic and military intelligence gathering." Westby explains that everybody is spying on everybody else, and says that "these countries are doing it to us, but were also doing it to them."[10] Since everyone is engaged in cyber espionage, the United States must focus on how it "can better coordinate the day-to-day defense, protection and operation of the department's computer networks."[11]

The" attacks" are not only against U.S. government and military targets; hackers also routinely target U.S. industry, including government contractors[12] and critical infrastructure.

"Attacks" against government contractors are typically attempts to steal trade secrets or other sensitive information (e.g. U.S. Government and military information), or to disrupt industry systems.

In January 2010, "hacker s"[13] (spies in this instance) targeted a variety of government contractors in a sophisticated and inventive attack that sent email invitations containing a PDF file that appeared to come from the Department of Defense. The email contained information about an actual event, adding credibility to the email. The exploit was a backdoor that connected to an IP address in Taiwan. The actual damage and/or information stolen is still to be determined.

Also, according to an investigation by the Wall Street Journal, hackers were able to steal terabytes of information about the Pentagon's $300 billion Joint Strike Fighter project, including detailed information about the aircraft's design which could expose vulnerabilities.[14] A Department of Defense Inspector General report found that "the advanced aviation and weapons technology for the JSF program may have been compromised by unauthorized access at facilities and in computers at BAE Systems, and incomplete contractor oversight may have increased the risk of unintended or deliberate release of information to foreign competitors". [15] Intruders copied and stole

[4] http://military.rightpundits.com/2009/07/08/north-korean-cyber-attack-widespread-computer-attack-on-us-government-agencies/
[5] http://www.defensenews.com/story.php?i=4425624
[6] http://www.federalnewsradio.com/?nid=15&sid=1816104
[7] http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111017588_pf.html
[8] Of course, one can assume the United States also attempts to gather information from other nations which could be used in the case of a conflict.
[9] http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111017588_pf.html
[10] http://content.usatoday.com/communities/technologylive/post/2010/01/chinese-cyberspies-arent-the-only-ones-on-the-prowl/1
[11] http://content.usatoday.com/communities/technologylive/post/2010/01/chinese-cyberspies-arent-the-only-ones-on-the-prowl/1
[12] Since the U.S. is not totally inept, do you ever wonder why some of this continues to go on… and whether some data is meant to be stolen… and the U.S. is giving as good as it is getting, or gaining more than it is losing?
[13] The term is used generically throughout this document. It may mean activists, criminals, nation-state spies, etc.
[14] http://www.pcworld.com/article/163533/fighter_jet_hack_far_from_first_government_breach.html
[15] http://www.pogo.org/pogo-files/alerts/national-security/ns-jsf-20090421.html

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

several terabytes of information about the design and electronic systems of the plane "potentially making it easier to defend against the craft".[16]

In addition to data loss associated with the Joint Strike Fighter project, plans for the VH-60N Marine One presidential helicopter were also found on a file server in Iran in the Spring of 2009.[17] Also, in 2008, after it was discovered hackers had breached the McCain and Obama campaign systems, a report found that Chinese hackers were able to gain access to the White House's email archives, and were able to sneak on to the network several times.[18]And in 2004, a group of Chinese hackers called "Titan Rain" were able to access sensitive information including military vehicle plans and the Army and Air Force's flight-planning software.[19, 20]

Given a single terabyte of information could take weeks to download, the intruders most likely had ongoing, constant access to the Defense Department computers,[21] although the hackers may have also accessed the information on a peer-to-peer network.[22] U.S. Air Force Lt. Gen. Robert Elder (Retired, July 2009) said that these kinds of attacks happen regularly, and that the military does focus on data loss because of attacks such as this.[23] This focus on preventing data loss likely equates to the military spending a considerable amount of their time and money trying to prevent intrusions into their networks. Going overboard with these efforts to stop data loss could begin to affect operations, such as the Pentagon ban on thumb drives. The military relied on thumb drives to store everything from operational instructions and manuals to medical records. Following the ban, transferring information became slower and soldiers had to use CDs and DVDs to perform system maintenance, although CDs and DVDs rarely withstand theater wear and tear.[24] Obviously, the threat is not only from data loss, but also from the risk that an enemy hacker could manipulate data. U.S. Air Force Lt. Gen. Robert Elder stated that while the focus is usually on data loss or data gain, our biggest concern should be that an adversary manipulates data and we do not even realize it.[25]

Early in 2009, hackers who are believed to be from Russia or China reportedly hacked the U.S. electrical grid and were able to install "software tools" that could disrupt the grid system. Investigators did not say how much of the grid had been accessed, but stated the attack was "pervasive" and could allow the hackers to take control of U.S. power plants.[26] The hackers reportedly wanted to be able to navigate and control the power grid as well as the water and sewage infrastructure.[27] Hackers would not even need to shut down the entire grid to cause damage. In 2008, the CIA reported that hackers had gained access to the networks of various utilities, causing power outages that affected multiple cities.[28] The new "smart grid" will be based on Internet technologies, meaning that it may be even more vulnerable to hackers. Utilities and plants actually will be completely connected.[29] Potential attackers could use grid system controls in the event of a war with them.[30] Security firm McAfee recently released a report, *In the Crossfire: Critical Infrastructure in the Age of Cyberwar*, which surveyed over 600 professionals responsible for critical infrastructure in 14 different countries, and found that 60 percent believed that foreign governments were involved in cyber attacks against their critical infrastructure. The McAfee report stated the most common

[16] http://www.pogo.org/pogo-files/alerts/national-security/ns-jsf-20090421.html
[17] http://www.nextgov.com/nextgov/ng_20090302_8335.php
[18] http://www.theregister.co.uk/2008/11/07/white_house_email_china/
[19] http://www.time.com/time/nation/article/0,8599,1098371,00.html
[20] http://www.pcworld.com/article/163533/fighter_jet_hack_far_from_first_government_breach.html
[21] http://www.computerworld.com/s/article/9131881/Report_Hackers_break_into_Pentagon_s_fighter_jet_project
[22] http://www.computerworld.com/s/article/9132571/Update_Strike_Fighter_data_was_leaked_on_P2P_network_in_2005_security_expert_says_
[23] http://www.aviationweek.com/aw/generic/story.jsp?id=news/THEFT042109.xml&headline=Report%20of%20F-35%20Data%20Theft%20Spotlights%20Flaws&channel=defense
[24] http://www.nextgov.com/nextgov/ng_20090217_6795.php
[25] http://www.aviationweek.com/aw/generic/story.jsp?id=news/THEFT042109.xml&headline=Report%20of%20F-35%20Data%20Theft%20Spotlights%20Flaws&channel=defense
[26] http://www.pcworld.com/article/162787/report_cybercriminals_have_penetrated_us_electrical_grid.html?tk=rel_news
[27] http://news.cnet.com/8301-11128_3-10214898-54.html
[28] http://www.securityfocus.com/brief/666
[29] http://www.greenercomputing.com/blog/2009/03/26/cia-hackers-have-already-attacked-electric-grid
[30] http://www.pcworld.com/article/163533/fighter_jet_hack_far_from_first_government_breach.html

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

type of "attack" were viruses or malware where the hackers had intent to steal financial information. These may better be considered "probes", although a third of the companies surveyed had experienced large-scale distributed denial-of-service attacks that had affected operations[31]. These may not be considered an attack in the traditional, kinetic attack sense of the word, but nor can they be classified as simply a probe since the intention was not to gain access or information, but to shut down services.[32]

Three U.S. oil companies were recently targeted in cyberattacks that experts say originated in China. Marathon Oil, ExxonMobil, and ConocoPhillips lost proprietary information including e-mail passwords, messages, and executive information including valuable discovery information which foreign companies can use to outbid U.S. oil companies.[33] The stolen information was sent back to a computer in China.[34] Foreign intelligence services increasingly target government contractors in order to access intellectual property[35]; and hackers are becoming better at creating highly-sophisticated social engineering attacks, which cannot be stopped by technology alone.

Web site defacements are also common. In January 2010, web site domain registrar and hosting provider Network Solutions reported that hackers had broken into their servers and defaced hundreds of customer Web sites. The hackers replaced each site's home page with anti-Israeli sentiments and pictures of militants with rocket launchers and rifles.[36] In January 2009, hackers defaced sites of the U.S. Army and the North Atlantic Treaty Organization, leaving the sites inoperable.[37] Following this attack, in February 2009, a hacker was able to break into the U.S. sales database of Kaspersky Lab, a highly regarded security engineering firm, and expose confidential customer and company information. The hackers also defaced the Web site, leaving the hacker identifier, "m0sted."[38]

The December 2009 attacks on Google, which are thought to have originated in China, have brought a lot of attention to cybersecurity. Google, as well as twenty other companies, were targeted in the attacks. Hackers apparently wanted access to Gmail accounts of Chinese human rights activists.[39] Google has said that the attack was "highly sophisticated and targeted" and announced that they may pull operations out of China. Leslie Harris, the president and CEO of the Center for Democracy and Technology, says that publicly announcing that they had been attacked, and taking action against the hackers, was a "bold and very difficult move on Google's part" but because of the "major cyber attacks aimed at human rights activists, it's hard to see how Google could have remained silent."[40]

Many experts claim that these attacks are not an isolated incident against Google, but rather "there's a raging, worldwide cyberwar going on behind the scenes."[41] Analysts say that multiple countries, in addition to China, have cyber capabilities, including friendly nations such as the United Kingdom or Israel, as well as less friendly nations including North Korea and Russia. Alan Paller, director of research at the SANS Institute, says that 100 countries have cyber espionage capabilities and that the Google incident represents the tip of the iceberg.[42] Admittedly, espionage is routinely accepted and nations such as China and Russia, as well as the United States, are reportedly bolstering their cyber espionage capabilities. War over an espionage attempt is unlikely. The fact is, many nations have cyber espionage capabilities, and there is a need to better secure systems and networks accordingly.

[31] http://www.v3.co.uk/v3/news/2256951/mcafee-warns-critical
[32] http://www.v3.co.uk/v3/news/2256951/mcafee-warns-critical
[33] The hackers gained access by using phishing emails that installed spyware on the victims' machines. Once a link in the "spear-phishing" email was clicked, a piece of advanced spyware was installed that can change digital signatures to avoid detection and find information. The hackers are given complete control of the network, and any data that is found is encrypted and sent back to the thieves.; http://www.axcessnews.com/index.php/articles/show/id/19305
[34] http://www.axcessnews.com/index.php/articles/show/id/19305
[35] http://www.thenewnewinternet.com/2010/02/03/the-chinese-are-coming-cyber-espionage-targets-government-contractors/
[36] http://www.krebsonsecurity.com/2010/01/hundreds-of-network-solutions-sites-hacked/
[37] http://www.theregister.co.uk/2009/01/10/army_nato_sites_defaced/
[38] http://news.techworld.com/security/110604/hacker-breaks-into-kaspersky-us-website/
[39] http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort
[40] http://www.computerworld.com/s/article/9144139/Google_threatens_to_leave_China_after_massive_cyberattacks
[41] http://www.foxnews.com/scitech/2010/01/22/google-vs-china-tip-cyberwar/
[42] http://www.foxnews.com/scitech/2010/01/22/google-vs-china-tip-cyberwar/

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

"Not a single NATO defense minister would define a cyber-attack as a clear military action at present."[43, 44]

With all of the focus on China' capabilities and espionage efforts, it is important to remember that China is also reportedly being hacked. The Web site of the Chinese Ministry of National Defense, for example, was attacked more than 2.3 million times within a month of going online.[45] According to Chinese foreign ministry spokesman Ma Zhaoxu, China is actually the biggest victim of cyber attacks.[46] China's largest search engine, Baidu.com, was taken offline because of attacks last month. For some time, the site displayed a message saying "This site has been hacked by Iranian Cyber Army," the same message that was posted on the Twitter site when it was attacked and shut down.[47] Experts say the attack most likely occurred because hackers modified Baidu's record with Registrar.com, a U.S. domain registrar.[48]

There have been several studies on U.S. cybersecurity policies and programs, and each have concluded in a list of recommendations usually including better public/private collaboration, better information sharing, increased international cooperation, and/or the creation of an international treaty. So far, the U.S. Government's progress has been minimal in addressing these recommendations.

Melissa Hathaway led a cybersecurity review starting in February 2009 which looked at the federal government's current cybersecurity programs and provided recommendations to the Obama administration for improving cybersecurity. One of the key recommendations from the review was to improve the federal government's partnership with the private sector. Hathaway writes, "There are many ways in which the Federal government can work with the private sector, and these alternatives should be explored. The public-private partnership for cybersecurity must evolve to define clearly the nature of the relationship, including the roles and responsibilities of each of the partners."[49]

In addition to Melissa Hathaway's federal cybersecurity review, the Center for Strategic and International Studies also released a report on federal cybersecurity, the Commission on Cybersecurity for the 44th Presidency. This report also emphasized the importance of a private and government partnership, saying , "the U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinate preventive and responsive activities."[50] Specifically, the report called for a presidential advisory committee including senior representatives from key cyber infrastructures; a townhall-style national stakeholders' organization that provides a platform for discussion; and a new operational center, the Center for Cybersecurity Operations, where public- and private-sector entities could share information on critical cybersecurity in a trusted environment.[51]

These reports are not alone in calling for better information sharing and partnership. Security experts and key people from industry have also called for better information sharing policies and programs. So far, it appears that these recommendations have been largely ignored.

[43] http://www.guardian.co.uk/world/2007/may/17/topstories3.russia
[44] This is part of the definitional problems – there are no international guidelines that define what constitutes a cyber "attack" and what is just espionage or probing. In the case of Estonia, a cyber attack was used along with a traditional invasion, yet NATO still could not classify the cyber attacks on Estonia as "military action". This highlights the need for a better international definition of cyber attack, cyber warfare, etc. At what point does cyber espionage become an attack? What amount of loss should be expected before military action can be taken?
[45] http://blogs.wsj.com/chinarealtime/2009/11/19/chinas-cyberwars/
[46] http://news.techworld.com/security/3210522/china-we-are-biggest-victim-of-hacking/
[47] http://www.computerworld.com/s/article/9143919/Group_behind_Twitter_hack_takes_down_Baidu.com
[48] http://www.computerworld.com/s/article/9144039/Baidu.com_probably_attacked_from_U.S._domain_registrar_says_researcher?taxonomyId=17
[49] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[50] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
[51] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

According to a Wall Street Journal report, "the U.S. government and private industry seem to be in a reactive role, detecting intrusions and information losses only after the fact, with no cross-government or industry coordinated response." The article goes on to say that "Efforts to coordinate standards and policies across the private sector and in government, therefore, appear stalled."[52] In addition, Computerworld reports: "The U.S. has no formal policy for dealing with foreign government-led threats against U.S. interests in cyberspace"[53] A report by the National Research Council, called *Technology, Policy, Law and Ethics regarding the U.S. Acquisition and Use of Cyberattack Capabilities,* cites three key points:

1. the U.S. policy and legal framework for the United States' use of cyberattacks is "ill-formed, undeveloped, and highly uncertain";
2. "the decision-making apparatus for cyberattack and the oversight mechanists for that apparatus are inadequate"; and
3. "secrecy has prevented us from being able to effectively share information and debate about the nature and implications of cyberattacks."[54]

In December 2009, the Homeland Security Department recently started an inter-agency initiative to create a National Cyber Incident Response plan which will "provide federal agencies, state and local governments, and the private sector with clear roles and responsibilities in case of a major attack". DHS says that the status quo is no longer sufficient in federal cybersecurity.[55]

In an interview with GovInfoSecurity.com in December 2009, Hathaway commented on the fact that the recommendation for a better public-private partnership has not been addressed. Hathaway said that "without bringing together the best of the government, with the best of the private sector, we are going to continue to be behind in that threat posture and security posture."[56] According to Hathaway, "It is important that we begin having a broader national dialogue of what is happening to our networks, both in the government and in the private sector and that we really start to translate it into what individuals can do, what corporations can do and what the government really needs to do to help secure our nation going forward."[57] Hathaway pointed out that most of our critical infrastructure is owned and operated by the private sector, and that the government must do a better job of sharing information with the private sector so that they know what is being targeted and what the threats are. With the proper incentives, the private sector can also help by increasing innovation and research and development.[58] The question is, why has the U.S. Government done so little since Hathaway's Spring 2009 report and recommendations?

Hathaway's federal cybersecurity review also called for the United States to cooperate more with other nations, saying "The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force."[59] Specifically, Hathaway writes that the U.S. government must develop "government positions for an international cybersecurity policy framework and

[52] http://online.wsj.com/article/SB10001424052748703399204574508413849779406.html
[53] http://fcw.com/articles/2010/01/25/buzz-google-china-ultimatum.aspx
[54] http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2110&zoneid=276
[55] http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221800388
[56] http://www.govinfosecurity.com/articles.php?art_id=1972
[57] http://www.govinfosecurity.com/articles.php?art_id=1972
[58] http://www.govinfosecurity.com/articles.php?art_id=1972&pg=2
[59] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

strengthen our international partnerships to create initiatives that address the full range of activities, policies and opportunities associated with cybersecurity."[60]

Several nations have proposed the idea of an international treaty with the United States, but the U.S. seems reluctant to discuss or commit to an international treaty. According to a study conducted last year by the U.S. Cyber Consequences Unit, "The international community urgently needs an organization to provide risk advisories on cyber threats and an international force to respond to cyberattacks against governments."[61] Sen. Dianne Feinstein (D-CA) says that an international treaty would give countries "built-in mutual assurances of behavior," but according to a report in the Wall Street Journal, "U.S. officials have in the past resisted such proposals out of concern that they would limit its options to maneuver, attack, and spy in cyberspace."[62] Another article claims that the United States has been rejecting requests from Russia to discuss cybersecurity for years.[63] The New York Times reported that the United States was in talks with the United Nations committee on disarmament, but the UN committee said that the United States has not contacted the committee to hold any talks. If the United States did talk with the committee on disarmament and international security, "it would be the first time as Washington has historically preferred to keep cyber security talks relegated to the UN committee on economics."[64]

Many are calling on the UN to become involved in cybersecurity. A post on the political hacking blog says that the U.N. is becoming involved in cyber, and that the U.N. believes that cyber weapons should be an issue for disarmament discussions. Early last year, UN secretary-general Ban Kimoon said that cyber weapons would be added to the list of arms that falls under the remit of the UN's Advisory Board on Disarmament Matters since critical system breaches are a threat to international security.[65] The United Nations also recently backed a conference of the High-Level Experts Group for the U.N.'s International Telecommunication Union's Cybersecurity Agenda. Experts from governments, the private sector, academia, research organizations and regional and international organizations participated in the conference, and discussed the need for international cooperation on cybersecurity. Participants agreed to lay the foundation for a UN anti-cybercrime agenda which focuses on legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation.[66]

This leads one to wonder,

Why is the United States notably absent in most international cybersecurity discussions?

and

Why does the international community so desperately want the U.S. to commit to a cyber "treaty"?

As former FBI CIO Zal Azmi says, "There have been a number of government cybersecurity plans put forward over the last several years…the plans have been gutted or otherwise disappeared off the public scene.[67] When it comes to cybersecurity, the time for talk is over and the time for action is way overdue…policies and procedures have been talked to death."[68]

[60] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[61] http://fcw.com/articles/2009/08/24/week-international-cyber-attack-fears.aspx
[62] http://online.wsj.com/article/SB10001424052748703338504575041680235626758.html
[63] http://www.spacewar.com/reports/US_Russia_begin_talks_on_cyberspace_security_report_999.html
[64] http://news.xinhuanet.com/english/2010-01/09/content_12779876.htm
[65] http://politicalhacking.blogspot.com/2009/03/un-concern-over-cyber-weapons.html
[66] http://www.un.org/apps/news/story.asp?NewsID=24221&Cr=cyber&Cr1=
[67] http://www.darkreading.com/security/government/showArticle.jhtml?articleID=222100083
[68] http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2167&zoneid=280

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

Maybe the U.S. Government has not been ignoring these studies and recommendations. Perhaps the U.S. Government has more advanced cyber capabilities than openly discussed, and perhaps they cannot fully support information sharing and international treaties without compromising their own capabilities and information gathering. For example, one of the goals of international cooperation, as well as public-private collaboration, is developing a way to attribute cyber attacks. The apparent lack of attribution[69] is routinely cited as a reason the U.S. Government is unable to authoritatively determine who is attacking U.S. infrastructure. On the surface, it seems that nothing has been done to address this critical attribution shortfall, and the U.S. Government has no way to firmly identify who is responsible for cyberspace attacks.

However, when Google's computer networks were attacked in December 2009, Google wasted no time in attributing the attacks (within 24 hours). Google even pinpointed the hackers as the "Honker Union," a group of Chinese hackers who claim to only defend Chinese websites.[70] Security researchers with Google were able to very quickly analyze the malicious software used in the attacks, the Hydraq Trojan, and find the source code for the algorithm of the malware, which pointed back to China.[71][72]

There are other cases where cyber attacks have been attributed. The recent attacks against oil companies Marathon Oil, ExxonMobil, and ConocoPhillips reportedly came from China. One of the oil company executives even called the breach the "China virus."[73] Data from the oil companies was easily traced to a computer in China, although some experts warn this could be another nation or cyberspy using Chinese servers to cover their tracks.[74] Russia was also quickly named as the source of attacks on the University of East Anglia's climate change department that resulted in the loss of confidential information. The emails were traced back to a computer company in Siberia, and while Chinese hackers were involved in the attacks, it was found that the emails were stolen by Russian hackers.[75] The UK's Office of Cyber Security says that it deals with attacks on government computer and key elements of national infrastructure that are coming from Russia and China every day.[76] The unit is able to attribute attacks back to Russia or China. It would appear that in some cases, groups are able to attribute attacks quickly and authoritatively, yet no one discusses how these attacks are attributed, and the U.S. Government continues to state "deterrence is further hampered by the significant issues surrounding the current and near term capabilities for definitive attribution."[77]

It is interesting that when Secretary of State Hillary Clinton spoke out about the Google attacks, she condemned China's policy of Internet censorship of their own people, while stopping short of condemning the hacking and espionage efforts against Google. While Clinton did ask for an investigation into the attack, she "singled out [China's] internet censorship as a threat to the freedom of information."[78] In her address following the attack, Clinton said that there was a "spike in threats to the free flow of information," although she did not discuss the actual attack on Google.[79] Clinton even met with Foreign Minister Yang Jiechi, but rather than discuss the attacks on Google, Clinton was expected to "press China's foreign minister on the issue of Internet freedom" and "unfettered Internet access around the world."[80]

---

[69] Not only is attribution a hindrance to deterrence and responding to a cyber threat, there is also the question of accountability. Can a nation or company be held accountable if an attack is able to get on to their systems / networks? What if they do not have (or reasonably enforce) the latest antivirus products installed, the latest patches and fixes installed? What if they do not properly follow industry norms for cybersecurity?

[70] http://www.benzinga.com/general/93085/google-suspects-honker-union-to-be-the-culprit-of-its-recent-cyber-attack-goog

[71] http://www.computerworld.com/s/article/9146239/Security_researcher_IDs_China_link_in_Google_hack

[72] No open source articles could be located that explain in detail how Google was able to attribute the attack to China. It is interesting to note that within a few days of the incident, media reports were published stating Google was partnering with the National Security Agency (NSA) to further investigate China's attacks.

[73] http://www.axcessnews.com/index.php/articles/show/id/19305

[74] http://www.axcessnews.com/index.php/articles/show/id/19305

[75] http://www.dailymail.co.uk/news/worldnews/article-1238638/Chinese-hackers-linked-Warmergate-climate-change-leaked-emails-controversy.html#ixzz0augDnCV0

[76] http://www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html

[77] http://defensetech.org/2010/02/01/cyber-attacks-a-law-enforcement-issue/

[78] http://www.telegraph.co.uk/technology/news/7104720/Hillary-Clinton-urges-Nato-to-tackle-cyber-terrorism.html

[79] http://www.foxnews.com/scitech/2010/01/21/clinton-address-internet-freedom-security/

[80] http://www.reuters.com/article/idUSTRE60Q34B20100127

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

The private sector, on the other hand, has made several efforts to secure cyberspace through partnerships amongst themselves and by developing ways to attribute attacks. The involvement of the U.S. Government in these efforts has been minimal.[81] Last year, for example, more than 20 companies partnered to combat the rapidly spreading Downadup worm. Participating companies included Microsoft, Symantec and Verisign, as well as ICANN, the nonprofit group that manages the Internet Domain Name System. Microsoft even offered a $250,000 reward for information about the hackers behind the worm.[82] Microsoft Security Response Center director Mike Reavey says that "the attacks are getting more complex, and if we want to get ahead of attackers the call is to work together in a community approach." Reavey also says that "customers want vendors to work together, and they want information and protection out faster."[83] U.S. Department of Homeland Security Secretary Janet Napolitano says that collaboration is necessary between the government, the public and the private sector. No one group can provide complete security, and Napolitano stresses the importance of user awareness and education in addition to public/private collaboration.[84] Where was the U.S. government (DHS, DOS, and/or DOD) in the industry collaboration and partnership?[85]

Could it be that the U.S. government, in action as opposed to merely words, resists international collaboration and sharing information with the private sector because intelligence gain/loss concerns?

An intelligence gain/loss assessment typically includes the warfighter determining whether the intelligence value of gaining information from a "target" is worth more than the value of destroying, or potentially compromising, that target. It seems logical intelligence gain/loss may be playing a significant role in the decisions of the U.S. Government regarding cyberspace security, as evidenced by the Secretary of Defense decision to place the National Security Agency in charge of US Cyber Command (USCYBERCOM). Even the Department of Homeland Security relies on the NSA to secure .gov networks.[86]

According to Jack Goldsmith, a Harvard Law School professor and member of the Hoover Institution's Task Force on National Security and Law, "The National Security Agency, the world's most powerful signals intelligence organization, is in the business of breaking into and extracting data from offshore enemy computer systems and engaging in computer attacks that, in the NSA's words, 'disrupt, deny, degrade or destroy the information' found in these systems."[87] Goldsmith went on to say that although the United States is not stealing intellectual property from democracy advocates like the Chinese, "we are aggressively using similar computer techniques for ends we deem worthy."[88, 89]

A series of documents released last year by the National Security Agency gave a description of how powerful the U.S. eavesdropping capabilities are, although the article did not say if American cyber warriors are currently hacking into foreign computer systems. As John Berthelsen, writing in the *Asia Sentinel*, says, "It may well be that

[81] Admittedly, some (many?) companies may not want to admit working / cooperating with the NSA because customers may be concerned regarding the privacy of their information. Reference http://www.wired.com/science/discoveries/news/2007/03/72811 for an example of NSA wiretapping, civil / privacy rights, etc. The more NSA involvement there is in private/industry cybersecurity, the more suspicion and concern over privacy rights there may be.
[82] http://www.computerworld.com/s/article/9127877/Microsoft_Symantec_VeriSign_join_forces_to_fight_Downadup_worm
[83] http://www.spacewar.com/reports/Teamwork_crucial_to_fighting_cyber_crime_Microsoft_999.html
[84] http://www.eweek.com/c/a/Security/DHS-Secretary-Stresses-CyberSecurity-Requires-Partnerships-User-Awareness-854958/
[85] A recent example of industry and government collaboration includes Google announcing it would work with the National Security Agency in order to better defend Google and its users from future attacks. The collaboration is meant to allow the NSA and Google to share critical information without violating Google's policies or laws that project users' privacy rights. Google is reportedly only sharing proprietary information with the NSA, not user searches or email accounts. "Achieving collaboration is not easy, in part because private companies do not trust the government to keep their secrets and in part because of concerns that collaboration could lead to continuous government monitoring of private communications"; http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html
[86] http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/
[87] http://asiasentinel.com/index.php?option=com_content&task=view&id=2284&Itemid=164
[88] http://asiasentinel.com/index.php?option=com_content&task=view&id=2284&Itemid=164
[89] If the U.S. agreed to an international agreement, it is possible they would be expected to act based on certain rules and guidelines, while other nations do not face or act according to similar constraints regarding cyber espionage, crimes, attack, etc.

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

American technological prowess is such, and other countries' defense means are so primitive, that they are never detected."[90] The NSA employs more than 60,000 people in intelligence, with an annual budget estimated at more than $10 billion.[91]

U.S. cyber forces are already deployed. Bob Gourley, who was the chief technology officer for the Defense Intelligence Agency and a board member of the Cyber Conflict Studies Association, says that U.S. cyber warriors are already "deployed overseas and are in direct contact with adversaries." Gourley says that these experts "live in adversary networks."[92] China has accused the United States of being more involved in cyberwar than we let on. In an editorial, the People's Daily said "U.S. intelligence agencies can, through technical means, fully monitor, follow and erase online information harmful to U.S. national interests."[93]

> *If collaboration with international partners and private industry is a sincere objective, why does the U.S. government want to put the NSA -- the very organization with the mission that includes spying, eavesdropping, and keeping some of the most secretive U.S. technical capabilities under wraps -- in charge of cybersecurity?*

Some have argued this is because the NSA has the government's largest and smartest collection of "geeks."[94] However,

> "possession of technical skills does not automatically equate to possession of warfighting skills. The computer science engineer would not be fully prepared for the cyberfight just because he or she understands networks. The traits required to be a warfighter go beyond the engineering skills obtained in school or the laboratory. Computer network exploitation experts might be excellent analysts and engineers who understand ways to defeat the adversary, but much more is involved -- integration with other operations, translation of effects to tasks, estimation of collateral damage, weaponization, standardization and assessment of combat and laws of armed conflict, etc. Cyberattack is not simply a "mouse click away" from computer network exploitation, and characterizing it as such is dangerous and reduces the commander's confidence that it will be done correctly."[95]

The same is true of day-to-day cyberspace operations. Exploitation and analysis capabilities, although abundant within NSA, do not equate to effective operations despite the fact that there are synergies to be gained between exploitation, attack, defense, and operations.

In a Spring 2009 essay, security expert Bruce Schneier said that "putting national cybersecurity in the hands of the NSA is an incredibly bad idea. An entire parade of people, ranging from former FBI director Louis Freeh to Microsoft's Trusted Computing Group Vice President and former Justice Department computer crime chief Scott Charney, have told Congress the same thing at this month's hearings." Schneier also discusses a "conflict on interest" that arises when the NSA is put in charge of cybersecurity. "Moreover, the NSA's dual mission of providing security and conducting surveillance means it has an inherent conflict of interest in cybersecurity. Inside the NSA, this is called the 'equities issue'. During the Cold War, it was easy; the NSA used its expertise to protect American military information and communications, and eavesdropped on Soviet information and

[90] http://asiasentinel.com/index.php?option=com_content&task=view&id=2284&Itemid=164
[91] http://asiasentinel.com/index.php?option=com_content&task=view&id=2284&Itemid=164
[92] http://www.nextgov.com/nextgov/ng_20091113_1728.php
[93] http://www.ft.com/cms/s/0/092d5ab6-08fc-11df-ba88-00144feabdc0.html
[94] http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/
[95] http://integrator.hanscom.af.mil/2007/June/06282007/06282007-14.htm

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

communications. But what happens when both the good guys the NSA wants to protect, and the bad guys the NSA wants to eavesdrop on, use the same systems? They all use Microsoft Windows, Oracle databases, Internet email, and Skype. When the NSA finds a vulnerability in one of those systems, does it alert the manufacturer and fix it -- making both the good guys and the bad guys more secure? Or does it keep quiet about the vulnerability and not tell anyone -- making it easier to spy on the bad guys but also keeping the good guys insecure? Programs like the NSA's warrantless wiretapping program have created additional vulnerabilities in our domestic telephone networks." Former DHS National Cyber Security division head Amit Yoran adds that "the intelligence community has always and will always prioritize its own collection efforts over the defensive and protection mission of our government's and nation's digital systems."[96]

Some argue that the NSA should oversee cybersecurity. Director of National Intelligence Admiral Dennis Blair recently told the House intelligence committee that "the National Security Agency has the greatest repository of cyber talent" and that "because of the offensive mission that they have, they're the ones who know best about what's coming back at us and its defenses against those sorts of things that we need to be able to build into wider and wider circles."[97] Paul Kurtz, who led the cybersecurity group on Obama's transition team and was part of Bush's White House National Security Council, recently told Forbes that the "NSA has the vast majority of expertise in information assurance inside the U.S. government," Kurtz said. "We have to tap that expertise while respecting privacy and civil liberties. I believe NSA can play a key role with proper oversight."[98]

Why would the U.S. Government give the intelligence collector (NSA) multiple responsibilities including cyber collection, exploitation, analysis, attack, defense, and operations?

> "Combining responsibilities is not effective when the tasks are potentially competing for priority and advocacy. In the case of the intelligence collector, the competition is the traditional one of intelligence gain/loss assessment, whereas the warfighter must decide whether the intelligence value of gaining information from a target is worth more than the value of destroying that target. In all operational scenarios, the final authority on intelligence gain/loss is the operational commander, who alone must accept the potential risks. However, if the authority also is the intelligence collector, the tendency will be to avoid any operations jeopardizing collection activities. This conflict will be exacerbated in a large organization. Even if the leader accepts the dual responsibility, the staff, who is devoted to collection, will continue to impede all other operations. The same holds true for the conflict between providing service and countering threats to the network. The emphasis always is placed on ensuring service availability while the threats often are dismissed because of a lack of tangible effects."[99]

It is far too easy to reach a conclusion that the U.S. government is not moving faster in securing cyberspace because, while the U.S. is in fact losing some data to international cyber espionage, the U.S., via NSA and/or other organizations, may actually be getting more than they are giving. Will "solving" attribution in fact allow others to point the finger at the U.S. in some international espionage cases? Will signing an international treaty tie the U.S.'s own hands? Will sharing more information between government and industry result in NSA capabilities (including tactics, techniques, and procedures) no longer being a national secret and/or industry being "tainted" due to NSA reputation (real or perceived)?

[96] http://www.schneier.com/essay-265.html
[97] http://www.wired.com/threatlevel/2009/02/nsa-should-over/
[98] http://www.wired.com/threatlevel/2009/02/nsa-should-over/
[99] http://integrator.hanscom.af.mil/2007/June/06282007/06282007-14.htm

Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee

While private industry, academia, and some international stakeholders appear to be taking specific actions to secure cyberspace[100], the U.S. government appears to be more of a cheerleader[101] than an on-the-field player. Is this part of an intentional strategy in the interest of intelligence gain/loss, or is the U.S. Government incapable of responding in a meaningful way due to bureaucratic obesity?

Regardless of the reason for U.S. Government cyber security inaction, a near-term challenge involves placing NSA (i.e., the Intelligence Community) in charge of CYBERCOM. [102] This is problematic from any perspective other than intelligence gain/loss and invites skepticism from the very stakeholders essential to improving cyberspace security - international partners, private industry, and military commanders. Collaboration and partnering with others will be essential regardless of who leads CYBERCOM and the centralization of U.S. cyberspace capabilities and resources. A "senior steering group" should be established[103] to help with deconflicting / synchronizing requirements and resources across the diverse group of cyberspace stakeholders. In addition, "cyber cells" should be established with stakeholder organizations to ensure stakeholders have access to the proper cyber expertise and information in support of their mission.

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

[100] Reference discussions earlier in this paper.
[101] http://www.staysafeonline.org is one example.
[102] Perhaps an alternative would be to leverage NSA as the Deputy Commander of US Cyber Command while appointing an operational 4-star, from other-than-the Intelligence Community, as the commander? NSA's authorities and resources could be applied to network collections / exploitation while other resources (e.g. DISA, USAF, USA, USN) could be applied to network defense, network attack, and network operations.
[103] Probably multiple versions of this senior steering group...for example: (1) DoD, (2) DoD + interagency, (3) DoD + interagency + industry, (4) DoD + interagency + industry + international

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578
Kathryn Stephens - kathryn.stephens@nsci-va.org ; Larry McKee